

CLAIMS:

1. A system comprising a plurality of devices, said plurality comprising at least a first device and a second device, the devices of said plurality being assigned a respective device identifier, the first device being arranged to authenticate itself to the second device by presenting to the second device a group certificate identifying a range of non-revoked device identifiers, said range encompassing the device identifier of the first device.
5
2. The system of claim 1, in which the respective device identifiers correspond to leaf nodes in a hierarchically ordered tree, and the group certificate identifies a node in the hierarchically ordered tree, said node representing a subtree in which the leaf nodes correspond to the range of non-revoked device identifiers.
10
3. The system of claim 2, in which the group certificate further identifies a further node in the subtree, said further node representing a further subtree in which the leaf nodes correspond to device identifiers excluded from the range of non-revoked device
15 identifiers.
4. The system of claim 1, in which the respective device identifiers are selected from a sequentially ordered range, and the group certificate identifies a subrange of the sequentially ordered range, said subrange encompassing the range of non-revoked device
20 identifiers.
5. The system of claim 1, further comprising a gateway device arranged to receive a group certificate from an external source and to distribute said received group certificate to the devices in the system if the device identifier of at least one device in the system falls within the particular range identified in said received group certificate.
25
6. The system of claim 5, the gateway device further being arranged to cache at least a subset of all the received group certificates.

7. The system of claim 1, in which a single group certificate identifies plural respective ranges of non-revoked device identifiers.

8. The system of claim 7, in which the plural respective ranges in the single group certificate are sequentially ordered, and the single group certificate identifies the plural respective ranges through an indication of the lowest and highest respective ranges in the sequential ordering.

9. The system of claim 1, in which the group certificate comprises an indication of a validity period and the second device authenticates the first device if said validity period is acceptable.

10. The system of claim 1, in which the second device is arranged to distribute protected content comprising an indication of a lowest acceptable certificate version to the first device upon successful authentication of the first device, and to successfully authenticate the first device if a version indication in the group certificate is at least equal to the indication of the lowest acceptable certificate version.

11. The system of claim 1, in which the second device is arranged to distribute protected content upon successful authentication of the first device, and to successfully authenticate the first device if a version indication in the group certificate is at least equal to the version indication in the group certificate of the second device.

12. A first device being assigned a device identifier, and being arranged to authenticate itself to a second device by presenting to the second device a group certificate identifying a range of non-revoked device identifiers, said range encompassing the device identifier of the first device.